

RECEIVED
CENTRAL FAX CENTER

NOV 01 2006

Serial No. 09/620,772

REMARKSI. Introduction

In response to the Office Action dated August 15, 2006, claim 1 has been amended. Claims 1, 2, 4-29 and 31-50 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for purposes of patentability.

III. Office Action Objections

In paragraph 4, the Office Action objects to claims 1 and 28 because the words "releasably coupleable" are misspelled. Also, in paragraph 5, the disclosure is objected to because the word "coupleable" is misspelled.

The Applicants have amended claim 1 to correct the spelling from "releaseably" to "releasably", but believe "coupleable" to be properly spelled. If the Examiner is aware of a reference describing a different spelling, the Applicants will gladly amend the claims and specification accordingly. The Applicants therefore traverse the objection as it pertains to the spelling of the word "coupleable".

IV. Non-Art Rejections

The Office Action rejected independent claims 1, 28, and dependent claims 2, 4-16, 43-46, and 29-41 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as his invention. The Examiner notes that no reference could be found in the specification for releasable coupleability.

The Applicants have amended the specification to include a reference in the specification for releasable coupleability. This amendment does not involve new matter, as releasable coupleability

Serial No. 09/620,772

was described in the claims in the disclosure as filed (see claim 27 of the instant application). Furthermore, the meaning of releasable is apparent from inspection (that which can be released) as is the meaning of "coupleable" (that which can be coupled).

V. The Cited References and the Subject Invention

A. The Okabe Reference

U.S. Patent No. 6,889,208, issued May 3, 2005 to Okabe et al. discloses a contents sale system. Original contents data are encrypted into encryption-resultant contents data in response to original playback key data. The original playback key data are encrypted into first encryption-resultant playback key data. The first encryption-resultant playback key data are encrypted into second encryption-resultant playback key data in response to an ID of a sale destination terminal apparatus. The encryption-resultant contents data and the second encryption-resultant playback key data are transmitted to the sale destination terminal apparatus. The sale destination terminal apparatus is enabled to decrypt the second encryption-resultant playback key data into the first encryption-resultant playback key data in response to the ID of the sale destination terminal apparatus. The sale destination terminal apparatus is enabled to decrypt the first encryption-resultant playback key data into the original playback key data. The sale destination terminal apparatus is enabled to decrypt the encryption-resultant contents data into the original contents data in response to the original playback key data.

B. The Akins Reference

U.S. Patent No. 6,560,340, issued May 6, 2003 to Akins et al. discloses a method and apparatus for geographically limiting service in a conditional access system. The cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

Serial No. 09/620,772

VI. Office Action Prior Art Rejections

In paragraph 10, the Office Action rejected claims 1, 2, 15, 17, 18, 25-29, 36, 40, 41 and 43 under 35 U.S.C. § 103(a) as unpatentable over Okabe. The Applicants respectfully traverse these rejections.

With Respect to Claims 1 and 28: Claim 1 recites:

A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:

- (a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;*
- (b) decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key;*
- (c) decrypting the program material using the first encryption key;*
- (d) re-encrypting the program material according to a second encryption key;*
- (e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and*
- (f) providing the re-encrypted program material and the fourth encryption key for storage.*

The Office Action acknowledges that the Okabe reference does not disclose the step of (e) *encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key*, but argues

"... '208 teaches "various means to incorporate a means of tracking the number of copies made of the content in col. 3, line 64 through col. 4, line 28; in addition '208 teaches "As shown in FIG. 3, the transfer control data contain four bits . . . representing a transfer generation number (a copy generation number) . . . Each time transferring or copying contents data is executed, the transfer-source player or apparatus (the copy-source player or apparatus) processes the transferred data or the copied data so that the number represented by the transfer-generation-number data piece is decremented by "1". When the transfer-generation-number data piece reaches "0000", transferring or copying contents data is prohibited. For example, the transfer-source player or apparatus (the copy-source player or apparatus) is disabled by the transfer-generation-number data piece being "0000" in col. 8, line 47 through col. 9, line 3."

"As well '208 teaches "The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which

Serial No. 09/620,772

will be used for data transfer or data copying to another player" in col. 7, lines 34-38 it is obvious by the text "other secondary encryption resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player" that as long as the transfer-generation-number contained in the header is not "000" that a new encryption key will be generated and included in the 'encryption-resultant playback key data'."

"As well '208 teaches "step 534 subsequent to the step S33 encrypts the primary encryption-resultant playback key data into other secondary encryption-resultant playback key data or third encryption-resultant playback key data in response to the ID of the copy-destination player (the transfer-destination player) 6b. A step S35 following the step S34 transmits the encryption-resultant contents data and the secondary encryption-resultant playback key data (generated by the step S34) to the copy-destination player 6b. The customer's player 6b recovers the original contents data as the customer's player 6a does (see FIG. 9). After the step S35, the current execution cycle of the program segment ends. The customer's player 6a is designed to upload the transfer control data representative of the transfer generation number (the copy generation number) to a host side each time the transfer generation number is updated." in col. 12, lines 25-48, this obviously would mean that each time the transfer generation number, and the encryption-resultant playback key data is updated, another key is generated, i.e. 'fourth encryption key', then fifth, sixth, etcetera."

The Applicants respectfully disagree that the Okabc reference discloses the features of claim

1. Claim 1 recites the step of

(a) *accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;*

Which the Office Action appears to analogize to the first player terminal apparatus receiving the primary encryption resultant playback key data and the encryption resultant contents data:

Serial No. 09/620,772

A customer's player 6a can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6a includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player 6a to implement processes mentioned later. The player 6a also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6a. In the case where the player 6a is connected with the terminal apparatus 5, the player 6a informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data.

Claim 1 then recites the step of

(b) *decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key*

Which the Office Action indicates is disclosed by the first player (6b) decrypting recovering the original contents data:

storage unit of the player 6a. The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

This is incorrect. The foregoing only discloses that the player recovers the original contents data by decrypting it. It does not disclose the step of decrypting the received access control information in a conditional access module to produce the first encryption key.

Claim 1 then recites the step of

(c) *decrypting the program material using the first encryption key;*

The Office Action indicates that this is disclosed as follows;

Serial No. 09/620,772

storage unit of the player 6a. The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other sec- 35

The foregoing indicates that the original contents data is recovered by decryption, but it does not indicate which key is used to accomplish this feat.

Claim 1 next recites:

(d) *re-encrypting the program material according to a second encryption key*

Analogizing this step to operations performed in player 6a, the Office Action indicates that this is disclosed in Okabe as follows:

storage unit of the player 6a. The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player. 35

This is incorrect. At no point does player 6a *re-encrypt* program material at all, nor does it do so with a *second key* different than the key by which it was encrypted when it was received by the player 6a (which the Office Action analogizes to Claim 1's "first key"). Instead, Okabe encrypts generates "other secondary encryption-resultant playback key data",

contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player. 35

and then sends that data, along with the same "encryption resultant contents data" that was received from the terminal apparatus 5 to the second player 6b.

Serial No. 09/620,772

player 6b. In the case where the player 6b is connected with the player 6a, the player 6b informs the player 6a of its own ID before contents data are transferred or copied. During the data transfer, the copy-source player 6a transmits the encryption-resultant contents data and the secondary 50 encryption-resultant playback key data into the storage unit of the copy-destination player (the transfer-destination player) 6b. Thus, the encryption-resultant contents data and the secondary encryption-resultant playback key data are copied. 55

Okabe therefore does not disclose step (d) of claim 1.

Steps (e) and (f) of claim 1 recite:

- (e) *encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and*
- (f) *providing the re-encrypted program material and the fourth encryption key for storage.*

The Office Action acknowledges that steps (e) and (f) are not disclosed in Okabe. This is plainly so, but not only for the reasons the Office Action suggests. Step (e) of claim 1 recites that the *second key*, which was used to *re-encrypt the program material* (a step that is not disclosed in Okabe) is then encrypted in the conditional access module according to a third encryption key to produce a fourth encryption key; and step (f) recites that this re-encrypted program material (and the fourth encryption key) is provided for storage. Since Okabe does not disclose re-encrypting the program material with a second key at all (it does not disclose step (d)), none of these steps can possibly be disclosed either.

Nonetheless, the Office Action argues:

- (1) That it would be obvious to modify Okabe to control the number of copies generated, and
- (2) That it would be obvious to do so by generating a new encryption key.

The Applicants disagree with both assertions. Okabe does not have to be modified to control the number of copies generated. Okabe does control the number of copies generated, and this is accomplished via a transfer generation number, which is part of the sale header, which is part

Serial No. 09/620,772

of the music-related data transferred from the terminal apparatus to the player 6a to the second player 6b. The Office Action asserts that Okabe discloses that "each time the transfer generation number, and the encryption resultant playback key data are updated, another key is generated", but the Applicants can find no part of Okabe that discloses this feature. Further, even if Okabe could be read this way, there is still no teaching to modify Okabe to perform step (d) of the Applicant's invention (re-encrypting the program material according to a second encryption key).

Okabe, in fact, teaches away from such a modification, because the "encryption resultant contents data" remains is never "re-encrypted" ... not by the terminal, not by the first player, nor by the second player. If it were to be decrypted and re-encrypted with a key, that key would have to be disseminated to each of the subsequent players, and Okabe surely does not provide a motivation for doing so or suggest how this might be done.

Claim 28 recites analogous features and is patentable for the same reasons.

With Respect to Claim 2, 15, 29, and 41: Claim 2 recites:

*The method of claim 1, wherein the encrypted access control information further comprises temporally-variant control data, and the method further comprises the steps of:
decrypting the received access control information to produce the temporally-variant control data; and
modifying the temporally variant control data to generate temporally-invariant control data.*

According to the Office Action, these steps are disclosed in Okabe as follows:

A customer's player 6a can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6a includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player 6a to implement processes mentioned later. The player 6a also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6a. In the case where the player 6a is connected with the terminal apparatus 5, the player 6a informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data.

Respectfully, the Applicants do not see where the notion of temporally variant and invariant control data is disclosed in any of the foregoing. Claim 29 recites analogous features and is patentable for the same reasons.

Serial No. 09/620,772

Claims 15 and 41 also recite that the control data is temporally-variant. The Office Action suggests that this feature is disclosed as follows:

ments data. In addition, the player 6a generates other sec- 35
ondary encryption-resultant playback key data (third
encryption-resultant playback key data) which will be used
for data transfer or data copying to another player.

but the Applicant respectfully disagrees, as no such disclosure is apparent.

With Respect to Claim 17: Claim 17 recites:

An apparatus for storing program material encrypted according to a first encryption key for replay, comprising:
a conditional access module, for accepting encrypted access control information including the first encryption key and temporally-variant control data, the control access module comprising:
a first decryption module, for decrypting the access control information to produce the first encryption key;
a first encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and
a second decryption module for decrypting the fourth encryption key to produce the second encryption key.

Claim 17 recites that the control data is temporally variant. The Applicants do not see where the Okabe reference discloses this feature as suggested by the Office Action:

A customer's player 6a can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6a includes a computer which operates in accordance with a 15
control program stored in a memory. The control program is designed to enable the player 6a to implement processes mentioned later. The player 6a also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6a. In the case where the 20
player 6a is connected with the terminal apparatus 5, the player 6a informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data. 25

Serial No. 09/620,772

Further, as described above, Okabe does not disclose anything equivalent to a second encryption key (because it does not decrypt the media program and re-encrypt it ... the second player passes the encrypted program material to the second player in the same form as it is received).

Finally, Okabe does not disclose anything like a second decryption module for decrypting the fourth encryption key to produce the second encryption key. That feature is not only undisclosed, Okabe plainly teaches against it. The whole point of Okabe is to transfer a program from the first player to the second ... it does not even remotely suggest transferring the same program from the second player back to the first as must be the case if the Office Action's analogies are adopted. Indeed, there would be no reason whatsoever to do so. That being the case, what motivation could there be for modifying Okabe to add a second decryption module for decrypting the fourth encryption key to produce the second encryption key?

With Respect to Claims 18: Claim 18 recites:

*The apparatus of claim 17, further comprising:
a tuner, communicatively coupleable to the conditional access module for receiving the encrypted access control information and the program material encrypted according to a first encryption key;
a third decryption module, for decrypting the program material using the first encryption key produced by the conditional access module;
a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and
a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key.*

As described above, Okabe does not disclose a second encryption module for re-encrypting the decrypted program material according to a second encryption key ... the encrypted media program is passed from the terminal to the first player to the second player without decryption and re-encryption. Also lacking is the fourth decryption module.

With Respect to Claim 25: Claim 25 recites that the second encryption key is stored in the conditional access module. The Office Action suggests that this is disclosed as follows:

Serial No. 09/620,772

A customer's player 6a can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6a includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player 6a to implement processes mentioned later. The player 6a also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6a. In the case where the player 6a is connected with the terminal apparatus 5, the player 6a informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data. The terminal apparatus 5 encrypts the primary encryption-resultant playback key data into secondary encryption-resultant playback key data (second encryption-resultant playback key data). In the case where the terminal apparatus 5 is connected with the player 6a, the terminal apparatus 5 downloads the encryption-resultant contents data and the secondary encryption-resultant playback key data into the storage unit of the player 6a. The player 6a recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6a generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

but nothing in the foregoing discloses the use of a second encryption key for re-encrypting the decrypted program.

In paragraph 11, the Office Action rejected claims 4-14, 16, 19-24, 31-35, 37-39, 42 and 44-50 under 35 U.S.C. § 103(a) as unpatentable over Okabe and Akins.

Applicants respectfully traverse these rejections.

With Respect to Claim 4: In rejecting the Applicants claims, the Office Action has analogized the "player" of the Okabe reference to a "conditional access module" and the "receiver" as the terminal. In rejecting claim 4, the Office Action now argues that it would be obvious that that "player" be a smartcard. In other words, that a smartcard be modified with all that is required to play a music program. In support of this proposition, the Office Action suggests that the motivation to do so would be to provide a more flexible means for distribute data. The Applicants

Serial No. 09/620,772

respectfully disagree. A smartcard is a small secure memory device who's primary utility lies in it being credit card sized, inexpensive, and operable without batteries. A smartcard cannot be used to play music without substantial modifications which are counter to the use for which smartcards are ordinarily put. Accordingly, the Applicant cannot agree that it is obvious to modify Okabe by making substituting a smartcard for the player.

With Respect to Claim 5: The Office Action suggests that the foregoing discloses that the access control information includes metadata describing at least one right for the program material:

50 instance 105. Control word 117 is produced by control word
generator 119 from information contained in entitlement
control message 107 and information from authorization
information 121 stored in set-top box 113. For example,
authorization information 121 may include a key for the
55 service and an indication of what programs in the service the
subscriber is entitled to watch. If the authorization informa-
tion 121 indicates that the subscriber is entitled to watch the
program of encrypted instance 105, control word generator
119 uses the key together with information from ECM 107
60 to generate control word 117. Of course, a new control word
is generated for each new ECM 107.

In fact, the foregoing discloses the opposite. It discloses that access control information is stored in the set top box, not in metadata transmitted with the access control information.

With Respect to Claim 10: Claim 10 recites the steps of retrieving the stored re-encrypted program material and the fourth encryption key, decrypting the fourth encryption key using the third encryption key to produce the second encryption key; and decrypting the re-encrypted material using the second encryption key. The Applicants respectfully disagree that Okabe can be modified as suggested by the Office Action.

The Office Action analogized the storage step of claim 1 to Okabe's storage of the program data in the second player. Nowhere does Okabe even remotely suggest that that data will be then retrieved by the first player from the second player. In fact, it strongly teaches away from this result. Accordingly, the Applicants cannot agree that there is any suggestion to modify as suggested.

Serial No. 09/620,772

With Respect to Claims 12, 13, 38, and 39: These claims recite details regarding the purchase of stored programs for replay. The Office Action suggests that these features are disclosed as follows:

- 50 instance 105. Control word 117 is produced by control word generator 119 from information contained in entitlement control message 107 and information from authorization information 121 stored in set-top box 113. For example, authorization information 121 may include a key for the
55 service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information 121 indicates that the subscriber is entitled to watch the program of encrypted instance 105, control word generator 119 uses the key together with information from ECM 107
60 to generate control word 117. Of course, a new control word is generated for each new ECM 107.

but the Applicants disagree. Further, Okabe discloses a paradigm wherein the program material is paid for and the right to replay is determined *before* the program material is downloaded. The Applicants believe that this paradigm is antithetical to that of Akins, and hence, there is no motivation to combine the references as suggested.

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference's disclosure will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the Applicant. *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994).

VII. Dependent Claims

Dependent claims 2, 4-16, 18-27, 29-42, and 43-50 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims

Serial No. 09/620,772

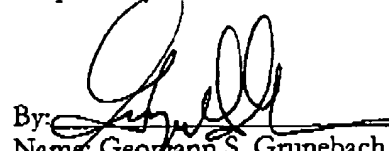
recite novel elements even more remote from the cited references. Accordingly, the Applicant respectfully requests that these claims be allowed as well.

VIII. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

Date: November 1, 2006

By: 
Name: Georgann S. Grunebach
Reg. No.: 33,179

The DIRECTV Group, Inc.
CA/LA1/A109
2230 E. Imperial Highway
P. O. Box 956
El Segundo CA 90245

Telephone No. (310) 964-4615